VITA Virginia Information Technologies Agency

Information Technology Security in Virginia

September 8, 2004

expect the best

Commonwealth of Virginia
Strategic Plan For Technology

- Design, develop, and implement a statewide security program and associated services
- Create a statewide information security office to include a cyber-incident response team and an IT security audit function
- Involve higher education in the statewide security program
- Develop evaluation tools for measuring cost savings

Today’s Computing Environment

Dependent upon vulnerable computer systems

- Emergency response, power grid, traffic controls, dam controls, train switching
- Criminal records, medical information
- Paychecks, social security and welfare checks, stocks, money transfers
- Federal Reserve transfers
- International wire transfers

find the security threat in this picture

The Security Threat

Hackers for Hire

Cyber Terrorism

Buffer Overflows

Session Hijacking

Hacktivism

Viruses

Worms

Replay Attack

Trojans

Proliferation of Hacker Tools

Port Scanning

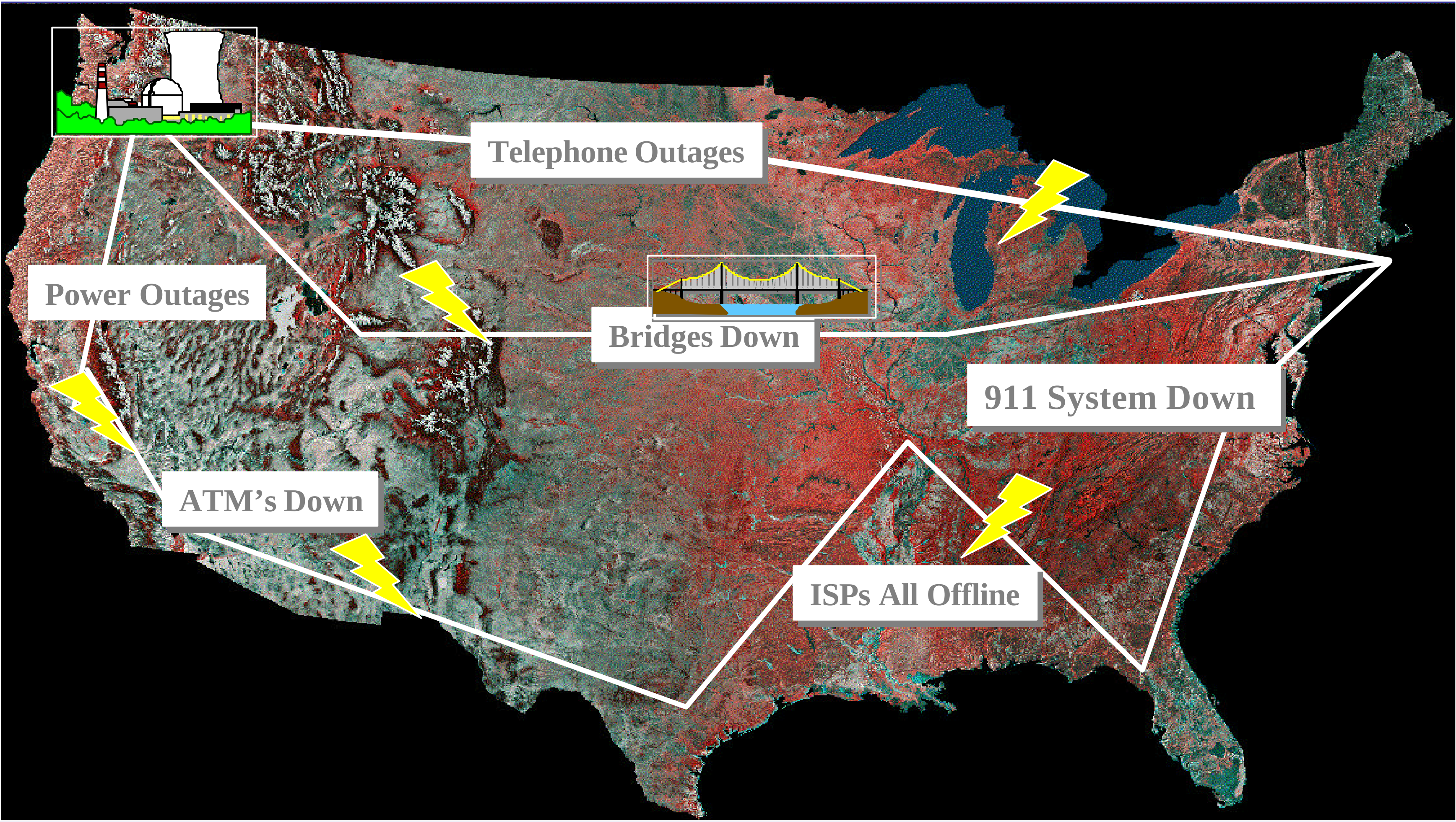
Denial of Service

Malicious Code

Spoofing

Man-in-the-middle

Imagine

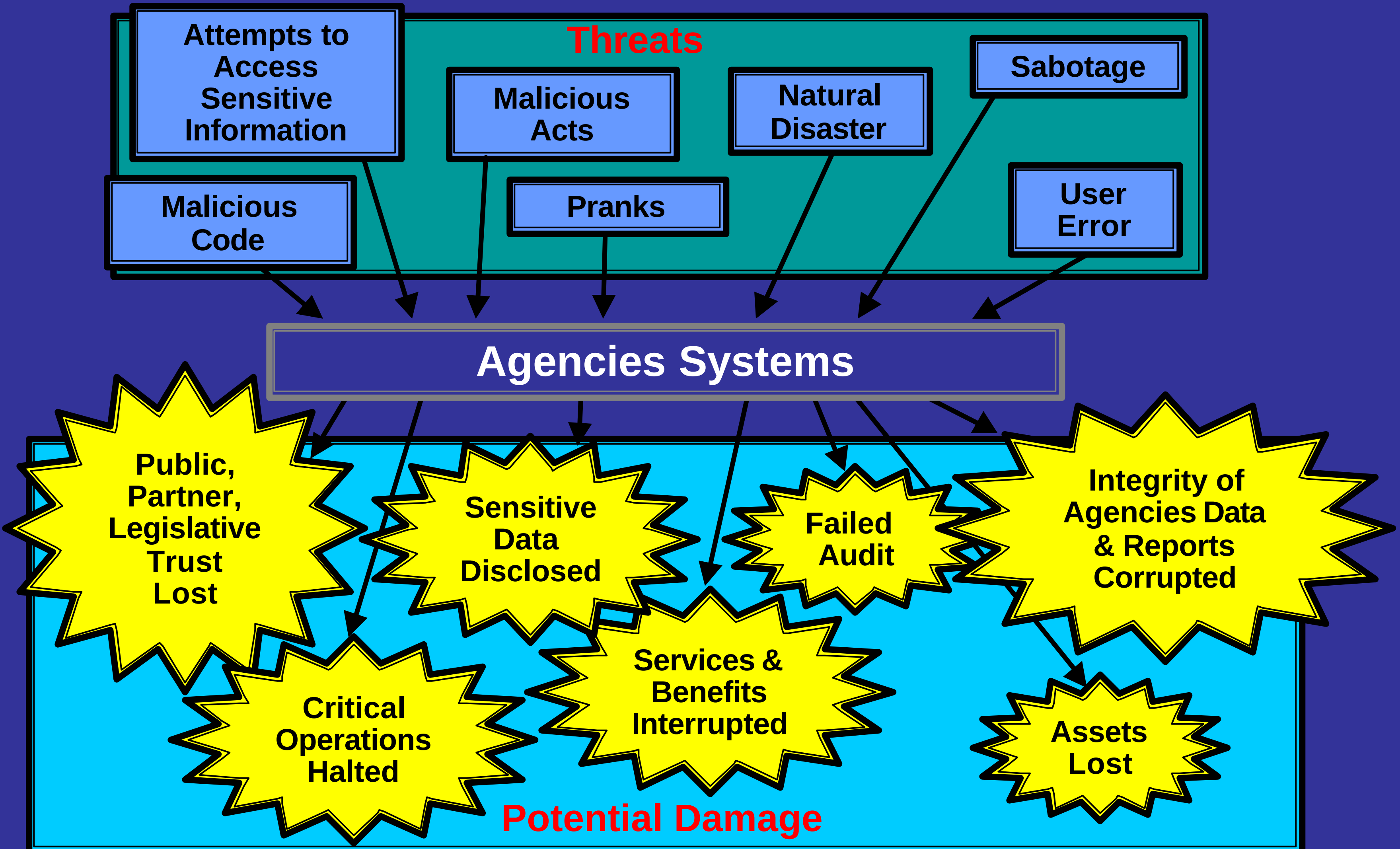


Unrelated events or strategic attack?

Risks Are Real

- Failure to comply with regulations
- Loss of public confidence
- Theft of sensitive information
- Financial fraud
- Liability issues
- Sabotage
- Espionage
- Malicious mischief

Enterprise Security Risks



Threats

Attempts to Access Sensitive Information

Malicious Acts

Natural Disaster

Sabotage

Malicious Code

Pranks

User Error

Agencies Systems

Public, Partner, Legislative Trust Lost

Sensitive Data Disclosed

Failed Audit

Integrity of Agencies Data & Reports Corrupted

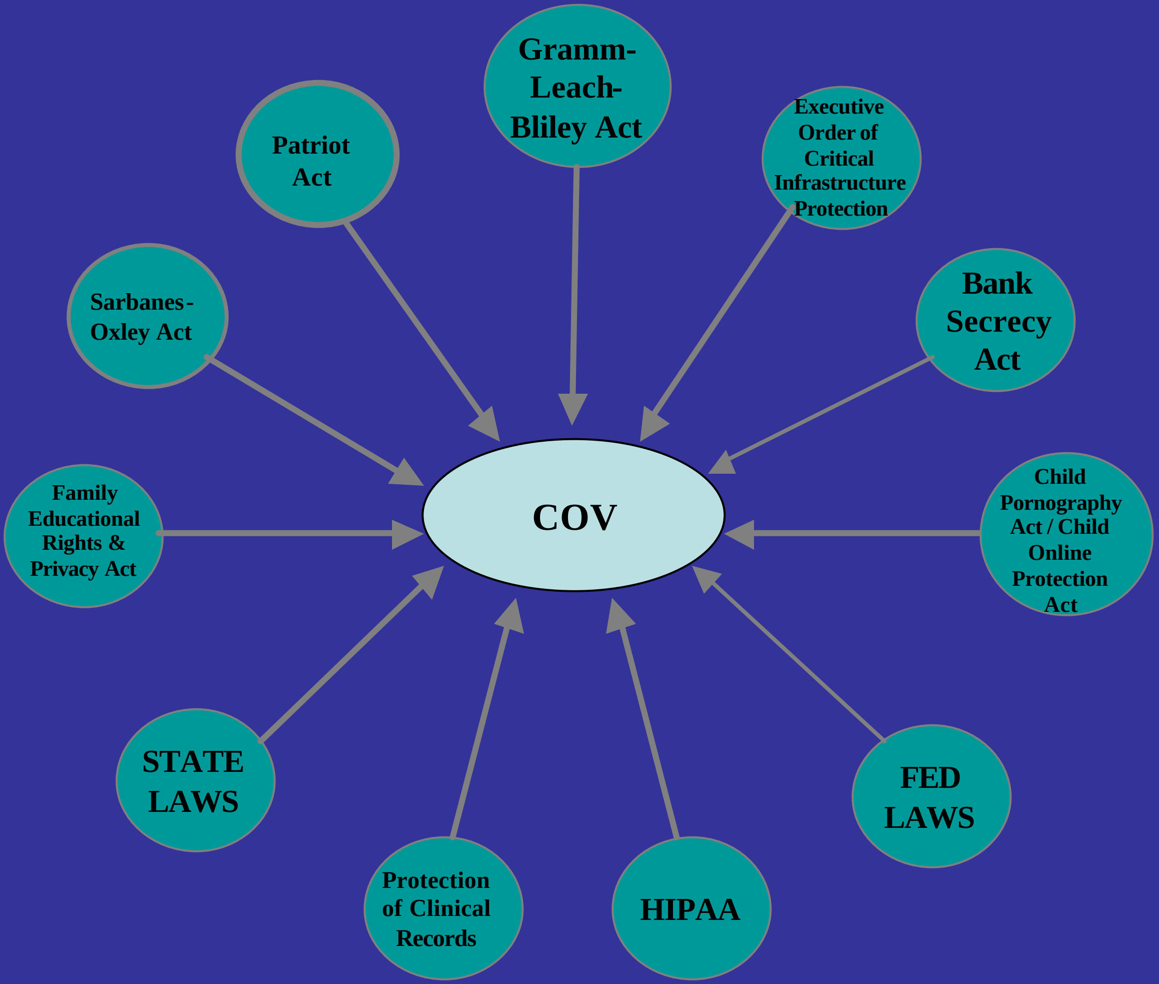
Critical Operations Halted

Services & Benefits Interrupted

Assets Lost

Potential Damage

Regulatory: Direct/Indirect Impact


Gramm-Leach-Bliley Act
Patriot Act
Executive Order of Critical Infrastructure Protection
Sarbanes-Oxley Act
Bank Secrecy Act
Family Educational Rights & Privacy Act
COV
Child Pornography Act / Child Online Protection Act
STATE LAWS
FED LAWS
Protection of Clinical Records
HIPAA

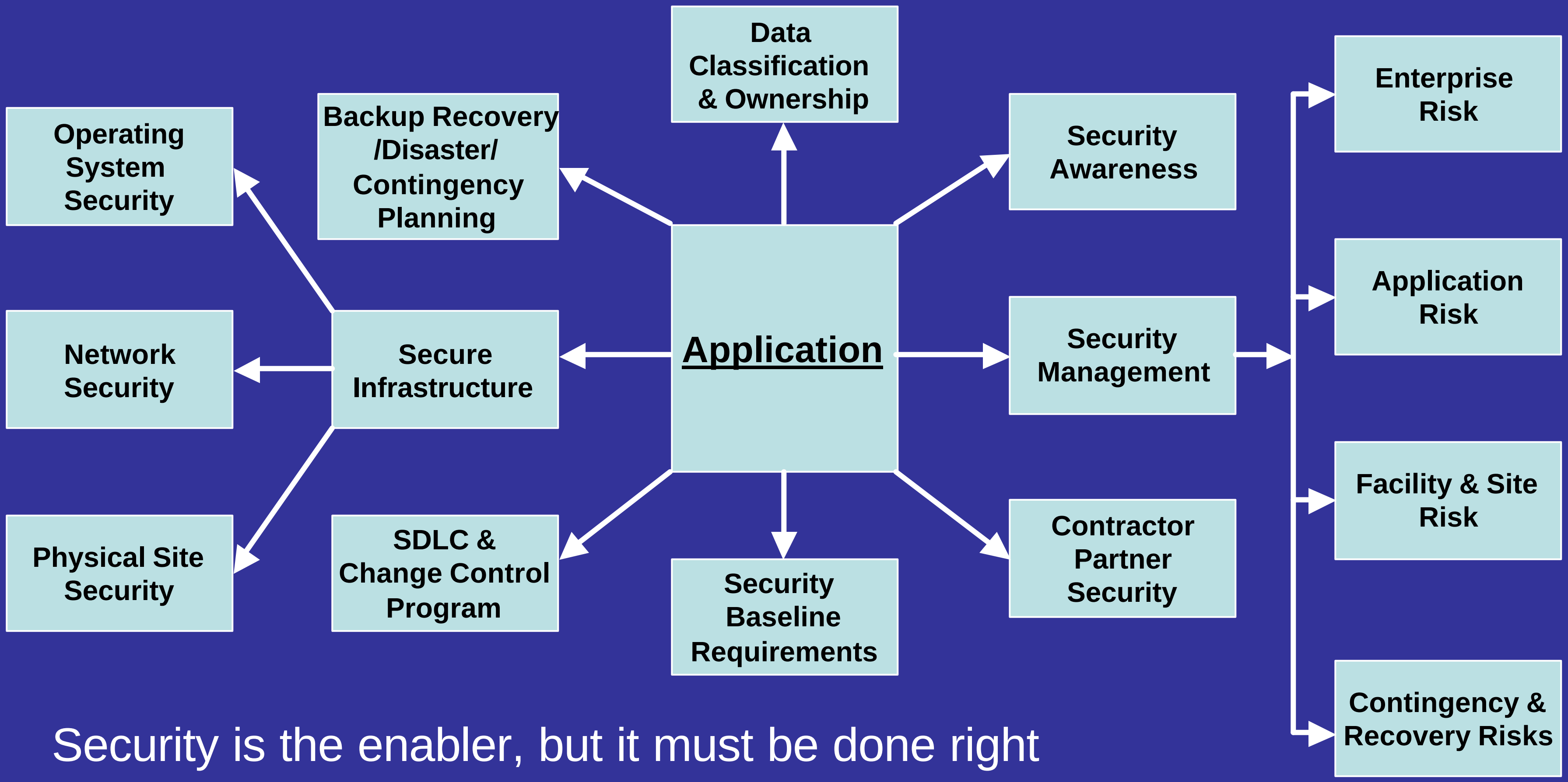
Commonwealth Security Challenges

- Security Requirements
- Vendors/Supply Chain Partners
- Products
- Internet and E-mail
- Reactive, not proactive
- Classification levels
- Overcoming the past
- Resources
- Getting security involved early
- Protect while allowing the user to function
- Promote security as an enabler, not an obstacle

Security Philosophy

- Basic Principles
  - Protect confidentiality, integrity, and availability
  - Security is a critical enabler
- Defense in Depth
- Enterprise Information Assurance
  - Protect and defend information and information systems
- Risk Management via defined process

Security Integration



Data Classification & Ownership

Operating System Security

Backup Recovery /Disaster/ Contingency Planning

Security Awareness

Enterprise Risk

Network Security

Secure Infrastructure

Application

Security Management

Application Risk

Physical Site Security

SDLC & Change Control Program

Security Baseline Requirements

Contractor Partner Security

Facility & Site Risk

Contingency & Recovery Risks

Security is the enabler, but it must be done right

Total Enterprise Security Solutions

Where We're Headed

- Enterprise Programs
  - Standards, Policies and Procedures
  - Secure Infrastructure and Technical Support
  - Critical Infrastructure Protection and Service Continuity
  - Risk Management
  - Information Security Training and Awareness
  - Incident Management

Where We're Headed

- Partnerships
  - Agencies
  - Higher Education
  - Contractors/Vendors
  - National Information Security Sources
  - Law Enforcement, FBI, Homeland Security
  - Other States

Statewide Security Office

Security Policies/ Procedures

Technology Standards

Economies of Scale

ENTERPRISE

Security Standards

Intrusion Detection

Security Training

Architecture

Incident Reporting

Turf Wars

Vision

Timeline

- Deployed in parallel to support the overall Program
- Enterprise Security Risk Assessment - 4/15/05

- Services:
  - Standards, Policies and Procedures - 1/31/05
  - Secure Infrastructure and Technical Support - 3/1/05
  - Critical Infrastructure and Business Continuity - 11/15/04
  - Risk Management - 6/1/05
  - Information Security Training and Awareness - 2/1/05
  - Incident Management

    Stage 1 - 11/30/04

    Stage 2 - 6/30/05

Contact Information

Jeff Deason, CISSP

Director of Security Services

Virginia Information Technologies Agency

jeff.deason@vita.virginia.gov